

Appl. No. 09/885,959

Amdt. Dated: May 19, 2005

Reply to Office Action of: November 19, 2004

REMARKS

The Applicant wishes to thank the Examiner for reviewing the present application.

Double Patenting

The Applicant notes the provisional rejection under the doctrine of obviousness-type double patenting in view of co-pending Application No. 09/931,013. However, the '013 application has been abandoned, and thus this objection is moot.

Claim Rejections

The Examiner rejected claims 8 and 17 under 35 U.S.C. 112, second paragraph, as being indefinite, based on improper antecedence for the expression "grouped terms  $G_i$ ". Claims 8 and 17 have been amended to indicate that the simultaneous multiple addition involves precomputing a value  $G_i$  representing a grouping of like elements as described on page 6, line 25 to page 7, line 10. Accordingly, claims 8 and 17 are submitted to comply with 35 U.S.C. 112, second paragraph.

The Examiner rejected claims 1-8, and 10-17 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,999,626 to Mullin. The Applicant respectfully disagrees.

The present invention is directed towards a method for improving the efficiency of multiplying an elliptic curve point  $Q$  with an integer  $k$ . In claim 1, the integer  $k$  is represented as a set of components  $k_i$ , such that  $k_i = \sum_i k_i \lambda_i$ , and this representation is used to obtain a value of  $kQ$  from  $k_0Q + k_1\psi(Q) + \dots$

Mullin teaches the application of the Frobenius operator to sets of precomputed points  $(k_i, k_iP)$  to compute a pair  $(k, kP)$ . Mullin starts with the sets  $(k_i, k_iP)$  a priori and ends with the computed point  $(k, kP)$  a posteriori. Mullin does not teach how to compute a scalar multiple of a point, but rather teaches how to derive a new point from an existing point, and how to derive the corresponding scalar multiple for the new point.

In the general embodiment of Mullin shown in Figure 3, the starting point is a key pair  $k_2, k_2P$  used to derive new values  $k_n, k_nP$ .  $k_nP$  is obtained by the application of the Frobenius operator to the point  $k_2P$ , and there is no contemplation of multiplying  $k_2P$  by another scalar  $k$  to

Appl. No. 09/885,959

Amdt. Dated: May 19, 2005

Reply to Office Action of: November 19, 2004

## BEST AVAILABLE COPY

obtain  $k_n P$ . In other words, figure 3 of Mullin does not suggest generating a new  $k$  and performing a scalar multiplication on a point. In fact, Mullin teaches independently deriving the new value of  $k$  through the use of  $\lambda_i$ , which in turn depends on the number of Frobenius operations performed on the point. However, the value of  $k$  computed is the scalar multiple of the seed point  $P$ , not the scalar multiple to get from  $k_2 P$  to  $k_n P$ .

The Examiner has referred to various passages in Mullin to support the above rejection. However, none of the passages cited suggest representing a scalar in the way recited in claim 1, and combining it with a point to generate a new point.

Moreover, the embodiment of Figure 4 of Mullin shows the combination of two points, namely  $k_1 P$  and  $k_2 P$ , to obtain a third point  $k_3 P$ . Again, however, there is no scalar multiplication of a point, simply a Frobenius operation and a point addition.

Accordingly, Mullin fails to teach a method of multiplying a point  $Q$  by a scalar  $k$ , or representing the scalar  $k$  in the form required in claim 1. Therefore, claim 1 is believed to clearly and patentably distinguish over Mullin. Claims 2-9 are either directly or indirectly dependent on claim 1, and as such are also believed to distinguish over Mullin.

Claim 10 is directed to a method which also involves generating a new  $k$  and performing a scalar multiplication on a point  $Q$ , and therefore, the arguments made in respect of claim 1 apply equally to claim 10. Claims 11-18 are directly or indirectly dependent on claim 10, and as such, are also believed to distinguish over Mullin.

The Examiner rejected claims 9 and 18 under 35 U.S.C. 103(a) as being unpatentable over Mullin in view of U.S. Patent No. 6,243,467 to Reiter. The Applicant respectfully disagrees.

In order for there a *prima facie* case of obviousness to be established, Reiter must at least teach, *inter alia*, the elements of the claims not taught by Mullin. The Applicants will show that Reiter does not teach generating a new  $k$  and performing a scalar multiplication on a point  $Q$ .

Reiter teaches computing  $kP$  for a given input integer  $k$  by using the Frobenius endomorphism  $\phi$  to write  $k = \sum_i k_i \phi^i$ . However, Reiter teaches the use of a decomposition algorithm that uses very specific properties of the Frobenius endomorphism. These properties do not hold for an arbitrary endomorphism.

Appl. No. 09/885,959

Amdt. Dated: May 19, 2005

Reply to Office Action of: November 19, 2004 **BEST AVAILABLE COPY**

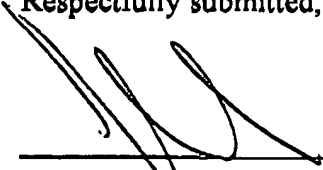
In particular, Reiter teaches decomposing a given integer  $k$  as  $k = \sum_i k_i \phi^i$  by repeated division by  $\tau$  in the ring  $Z[\tau]$ . The fundamental property is that an arbitrary element  $\gamma$  in  $Z[\tau]$  may be written as  $\gamma = q\tau + k$  in the ring, where the quotient  $q$  and the remainder  $k$  are in the ring, and  $N(k) < N(\tau)$ , where  $N$  is a Norm function in the ring. Continuing in this manner by dividing the quotient  $q$  by  $\tau$  often produces a representation of  $\gamma$  as  $\sum_i k_i \tau^i$  in the ring as desired.

Reiter, however, does not teach a method of multiplying a point  $Q$  by a scalar  $k$ , or representing the scalar  $k$  in the form required in claim 1. Therefore, Reiter does not teach the missing elements from Mullin, and as such, claims 1-18 are believed to be patentable over the combination of Mullin and Reiter.

Accordingly, the Applicants believe that claims 1-18 clearly and patentably distinguish over Mullin, and the combination of Mullin and Reiter, and as such, are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

  
\_\_\_\_\_  
John R.S. Orange  
Agent for Applicant  
Registration No. 29,725

Date: May 19, 2005

JRO/BSL